LEOSTREAM™ ◯

REMOTE ACCESS FOR ALL
User connections to anything – anytime, anywhere, from any device.

Quick Start with Leostream

Provide Remote Access and Desktop Connection Management for Hybrid Clouds

Version 9.1
October 2021

Contacting Leostream

Leostream Corporation   http://www.leostream.com
271 Waverley Oaks Rd.   Telephone: +1 781 890 2019
Suite 204
Waltham, MA 02452
USA

To submit an enhancement request, email features@leostream.com.
To request product information or inquire about our future direction, email sales@leostream.com.

Copyright

Trademarks

Patents

Leostream software is protected by U.S. Patent 8,417,796.

Contents

Overview

The Leostream Connection Broker lies at the heart of any hosted desktop deployment, and is the key component for provisioning resources in the cloud, assigning and connecting end users to resources, and managing the end user's remote session. The Connection Broker provides end users with consistent, reliable access to desktops hosted in a variety of on-premises and public cloud platforms, from a wide range of client devices.

The Connection Broker is configured using the Administrator Web interface, where you define the Leostream concepts that control your environment. For more information on Leostream concepts, see the Introduction to the Leostream Platform guide.

The following procedure steps you through a general Connection Broker configuration. It assumes you already installed and licensed your Leostream Connection Broker, and installed Leostream Agents on your remote desktops. For information on installing and licensing the Leostream components, see the Leostream Installation Guide.

Integrating with Your Existing Infrastructure

In the **Setup** section of the Connection Broker Administrator Web interface, you integrate Leostream with the other components of your hosted desktop environment, such as your Microsoft Active Directory authentication servers and the virtualization or cloud platforms that host your desktops.

The **Setup** section is also used to integrate your Connection Broker with the Leostream Gateway. Note that this Quick Start guide does not cover using the Leostream Gateway. For more information on configuring your Connection Broker to work with the Leostream Gateway, see the Leostream Gateway Guide.

Adding Authentication Servers

The Connection Broker can authenticate users in standard LDAP systems, such as Active Directory, or OpenLDAP™, and with NIS authentication servers. In this example, we add an Active Directory authentication server, as follows.

Note: Any options not covered in the following procedure remain at their default values.

1. Navigate to the **> Setup > Authentication Servers** menu.

2. Click the **Add Authentication Server** link, shown in the following figure.

3. The **Add Authentication Server** form opens. In the **Authentication Server name** edit field, enter a name for this server in the Connection Broker.

4. In the **Domain** edit field, enter the domain name associated with this Active Directory server.

5. In the **Connection Settings** section, shown in the following figure, use the following procedure to integrate with your Active Directory authentication server.

a. Select **Active Directory** from the **Type** drop-down list.

b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.

c. Enter the authentication server hostname or IP address in the **Hostname or IP address** edit field.

d. Enter the port number in the **Port** edit field.

    If you have a multi-domain forest and need to search the global catalog to locate users across the domains, you must use the default Global Catalog port. Modify the **Port** field to use 3268 for LDAP and 3269 for LDAPS.

e. Check the **Encrypt connection to authentication server using SSL (LDAPS)** checkbox if you need a secure connection to the authentication server. The port number automatically changes to 636. Re-edit the **Port** edit field if you are not using port 636 for secure connections.

5

6. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read access to the user records. Leostream does not need full administrator rights to your Active Directory authentication server.
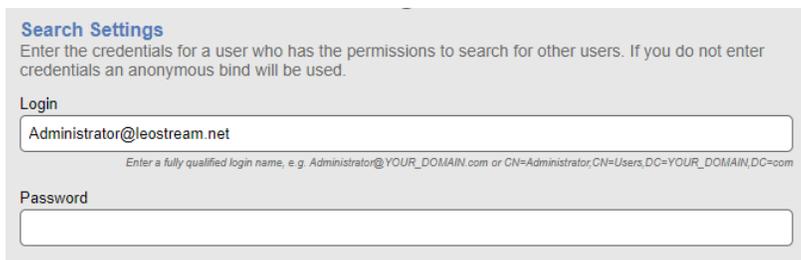
Search Settings
Enter the credentials for a user who has the permissions to search for other users. If you do not enter credentials an anonymous bind will be used.

Login

Administrator@leostream.net

Enter a fully qualified login name, e.g. Administrator@YOUR_DOMAIN.com or CN=Administrator,CN=Users,DC=YOUR_DOMAIN,DC=com

Password

7. In the **User Login Search** section, ensure that the **Match Login name against this field** edit field is set to **sAMAccountName**. This is the attribute that the Connection Broker uses to locate the user in the authentication server, based on the information the user enters when logging into Leostream.

8. Click **Save**.

For more detailed instructions, see the chapter "Authenticating Users" in the [Connection Broker Administrator's Guide](#).

Defining Centers to Communicate with Hosting Platforms

The Connection Broker interfaces with a number of virtualization and cloud platforms, allowing you to build a hybrid-cloud environment for your hosted desktops and applications.

💡 *Leostream defines **centers** as the external, third-party platforms that host your desktops. The Connection Broker interacts with these centers to inventory desktops available for assignment to end users, as well as to provision and delete desktops based on demand.*

In this example, virtual machines are hosted in VMware vSphere, and vSphere is managed by VMware vCenter Server. For the Connection Broker to manage these machines, define a *center* for vCenter Server, as follows. For details on defining centers when not using VMware, see the "Creating Centers" section of the [Connection Broker Administrator's Guide](#).

1. Navigate to the **> Setup > Centers** menu.

2. Click the **Add Center** link, as shown in the following figure.
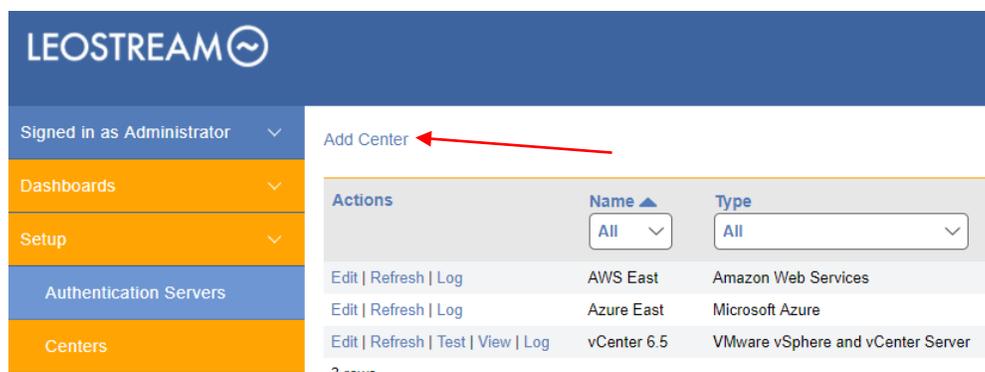
3. Configure the **Add Center** form, as follows:

   a. Select VMware vSphere and vCenter Server from the **Type** drop-down, as shown in the following figure.

💡 *Your Connection Broker license determines which hosting platforms you can integrate with your Connection Broker. If the hosting platform you want to use is not listed in the **Type** drop-down menu, please contact sales@leostream.com to obtain an updated license key.*

b. Enter a name for the center in the **Name** edit field.

c. Enter the vCenter Server's address in the **Hostname or IP address** edit field.

d. In the **Username** edit field, enter the name of a user with the necessary privileges.

e. Enter this user's password into the **Password** edit field.

f. Click **Save**.

For full instructions, see the "VMware vSphere and vCenter Server" section in Chapter 6 of the Connection Broker Administrator's Guide.

If your vCenter Server manages a large number of machines, refreshing the center can place a substantial load on vCenter Server. If you are experiencing responsiveness issues, try increasing the refresh interval.

Leostream requires specific VMware vCenter Server privileges in order to perform various actions, such as starting and stopping VMs, or provisioning new virtual machines. If your Connection Broker is unable to perform any of these actions, ensure that you create your center with an account that has all the required privileges. You can use the **Test** action associated with your saved VMware center to see what privileges are assigned to the user associated with this center.

To see the virtual machines inventoried from this center, navigate to the **> Resources** > **Desktops** page. See the "Working with Desktops" section of the Connection Broker Administrator's Guide for information on viewing, editing, and controlling desktops from within the Connection Broker.

Configuring Your Connection Broker

In the **Configuration** section of the Connection Broker Administrator Web interface, you define the pools, plans, and policies that determine which users have access to which desktops, how they are connected, and how the Connection Broker manages the user's session.

Step 1: Creating Pools

After you create your centers and the Connection Broker inventories your desktops, you logically group the desktops into *pools*. Use pools to create sets of desktops that you want to offer to particular groups of users, or to group desktops that are administrated by particular individuals.

*The Leostream Connection Broker defines a **pool** as a group of desktops. Desktops can be members of multiple pools. How the Connection Broker manages the user's connection to a desktop is determined by the pool it is offered from.*

Leostream provides a number of flexible methods for creating pools. For a complete description, see the "Creating Desktop Pools" chapter in the [Connection Broker Administrator's Guide](). In this example, we'll create a pool of all of the Microsoft Windows virtual machines in the vSphere center created in the previous chapter.

1. Navigate to **> Configuration > Pools** menu.

2. Click the **Create Pool** link, shown in the following figure.
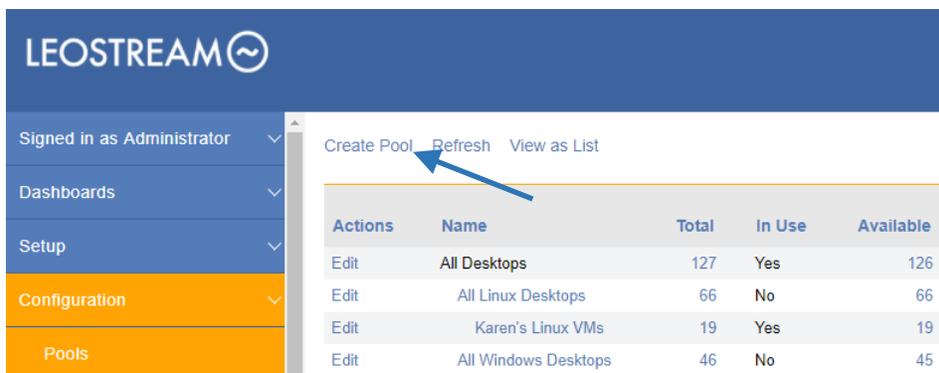
3. In the **Create Pool** form that open, enter a unique name for this pool in the **Name** edit field.

4. From the **Subset of pool** drop-down menu, select **All Windows Desktops**.

5. Select **Centers** from the **Define pool using** drop-down menu.

6. From the **Available centers** list, select your vCenter Server center.

7. Click the **Add items** link to the right of the **Available centers** list. The VMware center should now be listed in the **Selected centers** list.

8. Click **Save**.

Step 2: Defining Pool-Based Plans

After you separate your desktops into pools, define the rules that control how the Connection Broker manages the user's connection to the desktops in those pools. To perform this step, ask yourself the following questions.
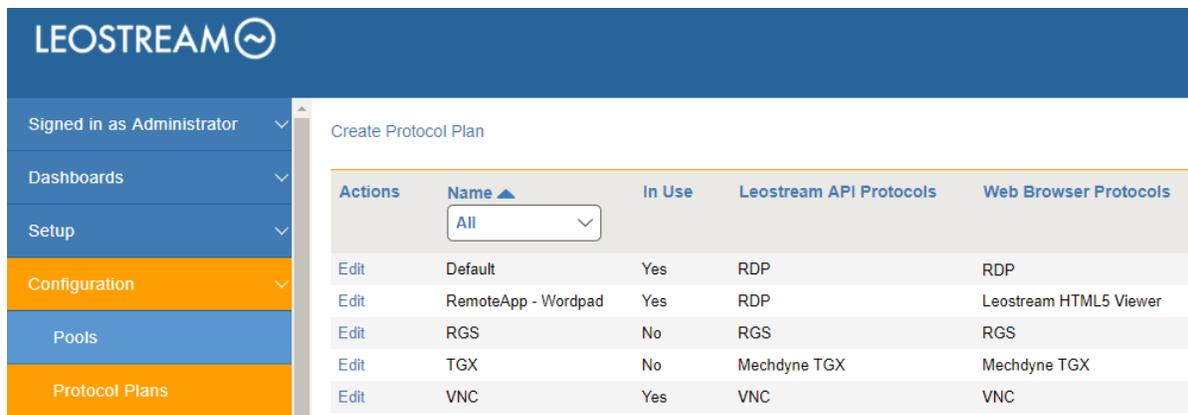
- What display protocols do I want to use to connect users to their desktops?
- How do I want to manage the power state of each desktop, for example, should it be powered off when the user logs out?

- How long can users remain assigned to a particular desktop? For example, if the user logs out, should they remain assigned to that desktop, or should another user be able to log in?

💡 *The Leostream Connection Broker defines a **pool-based plan** as a set of rules that determine how the Connection Broker manages the connection to a desktop in a pool. This step describes three types of pool-based plans. 1) Protocol, 2) Power Control, and 3) Release. The Connection Broker also provides **location-based plans** for setting registry keys and attaching network printers to the remote desktop. See the Connection Broker Administrator's Guide for information on using location-based plans.*

Protocol Plans

Protocol plans determine the display protocol the Connection Broker uses to connect a user to their desktop. The Connection Broker provides one default protocol plan, which is shown on the **> Configuration > Protocol Plans** page, shown in the following figure.

The default Protocol Plan instructs the Connection Broker to connect to the remote desktops using Microsoft RDP.

To create a new Protocol Plan, click the **Create Protocol Plan** link. The **Create Protocol Plan** form is divided into sections based on the type of client device used to log into Leostream, for example, Leostream Connect or the Leostream Web client.

💡 *Your Connection Broker license determines which display protocols your Connection Broker can use. If the display protocol you want to use is not shown on the **Create Protocol Plan**, please contact sales@leostream.com to obtain an updated license key.*

In each section, indicate which protocol the Connection Broker should use to connect users to their desktops by selecting **1** from that protocol's **Priority** drop-down menu. Then, use the **Configuration file** and **Command line parameters** to determine how that connection is launched. For example, for RDP, the **Configuration file** is a list of RDP-file parameters that determine if, for example, the connection is launched in full screen.

💡 *See the Leostream Guide for [Working with Display Protocols](#) for more information on defining command line parameters and configuration files for each supported display protocol.*

For this example, we'll use the Default protocol plan to launch RDP connections to our pool of Windows desktops. For a complete description of protocol plans, see "Building Pool-Based Plans" in the [Connection Broker Administrator's Guide](#).
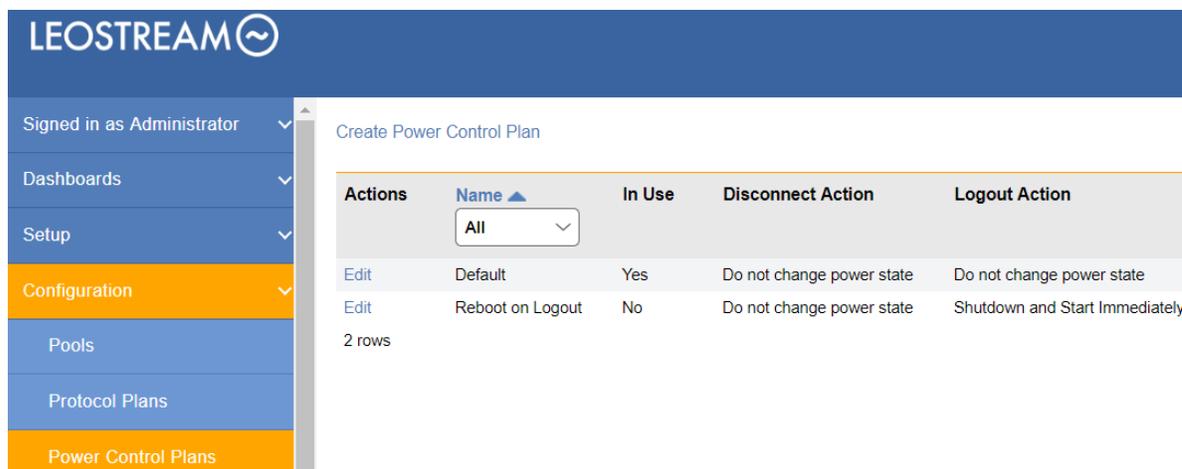
Power Control Plans

Power control and release plans allow you to take actions on the user's remote session based on different events, such as:

- When the user disconnects from their desktop
- When the user logs out of their desktop
- When the desktop is released to its pool
- When the user's session has been idle for a specified length of time (not supported for multi-user RDS or Linux sessions.)

⚠️ *The remote desktop must have an installed and running Leostream Agent to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.*

Power control plans define the power control action to take on a desktop. Available power control plans are shown on the **> Configuration > Power Control Plans** page, shown in the following figure.

Actions	Name ▲	In Use	Disconnect Action	Logout Action
	All ▾			
Edit	Default	Yes	Do not change power state	Do not change power state
Edit	Reboot on Logout	No	Do not change power state	Shutdown and Start Immediately

2 rows

11

New Connection Broker installations contain one default power control plan, called **Default**. You can create as many additional power control plans as needed for your deployment. To build a new power control plan:

1. Click the **Create Power Control Plan** link on the **> Configuration > Power Control Plans** page. The **Create Power Control Plan** form, shown in the following figure, opens.

Enter a descriptive name. You'll refer to this name when assigning the plan to a pool.

Select the amount of time to wait before changing the desktop's power state. A wait time of zero tells the Connection Broker to immediately execute the selected power control action.

Select the power control action to take after the wait time elapses. For the Connection Broker to take actions based on disconnect or idle-time events, you must install the Leostream Agent on that desktop.

2. Enter a unique name for the plan in the **Plan name** edit field.

3. For each of the remaining sections:

    a. From the **Wait** drop-down menu, select the time to wait before applying the power action.

    b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.

4. Click **Save** to store the changes, or **Cancel** to return to the **> Configuration > Power Control Plans** page without creating the plan.

Release Plans

Release plans determine how long a desktop remains assigned to a user. When the assignment is broken, the Connection Broker releases the desktop back to its pool, making it available for other users. Available release plans are shown on the **> Configuration > Release Plans** page, shown in the following figure.

💡 *When a desktop is **assigned** to a user, the Connection Broker always offers that desktop to that user, regardless of where the user logs in, and to no other users. Desktops can be policy-assigned or hard-assigned. For a description of hard-assigned desktops, see the Connection Broker Administrator's Guide.*
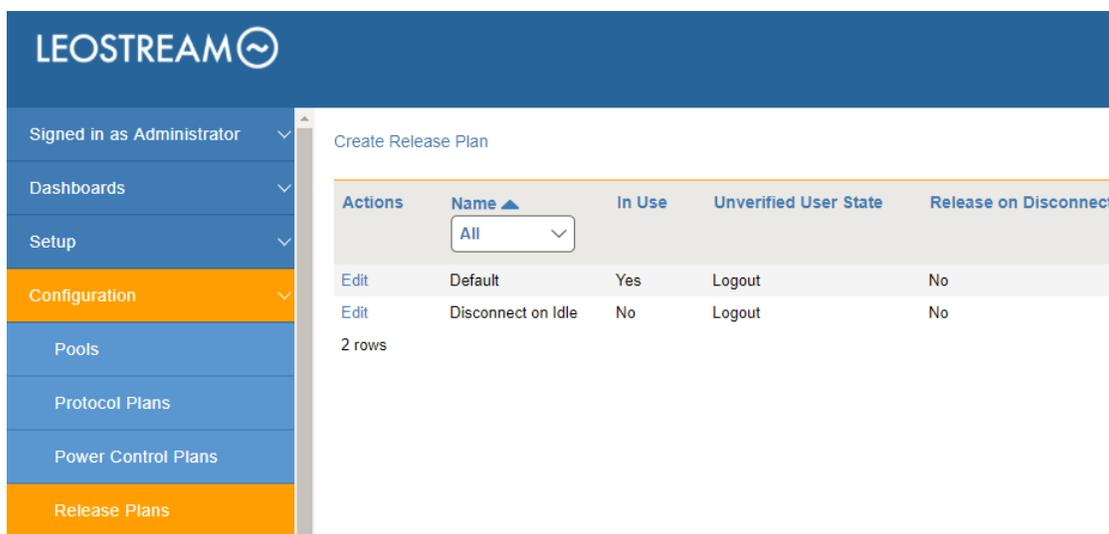
New Connection Broker installations contain one default release plan. The default release plan is designed to keep the user assigned to their desktop until they log out. When the user logs out, the Connection Broker releases the desktop back to its pool. You can create as many additional release plans as needed for your deployment.

For this example, we build a release plan that schedules a logout one hour after the user disconnects from their desktop:

1. Click the **Create Release Plan** link on the **> Configuration > Release Plans** page. The **Create Release Plan** form, shown in the following figure, opens. The figure describes additional use cases you can model using Release Plans.

Create Release Plan

Plan name

When User Disconnects from Desktop

Release to pool: No

Log user out: After 1 hour

URL to call

When User Logs Out of Desktop

Release to pool: Immediately

URL to call

When Connection is Closed

Execute actions for: When User Logs Out of Desktop

This section of the plan executes when a Leostream Agent is installed or communicating on the remote desktop

When Desktop is Idle

Lock desktop: No

Disconnect: No

Log user out: No

When Desktop is First Assigned

Release to pool: No

Release if user does not log in: No

"When Desktop is Released" actions will not be invoked

When Desktop is Released

☐ Log user out of the desktop

Delete virtual machine from disk: No

Annotations:

Enter a descriptive name. Refer to this name when assigning this plan to pools.

To model a persistent desktop, ensure that the desktop is not released when the user disconnects or logs out.

If a Leostream Agent is not installed on the remote desktop, the Connection Broker cannot distinguish when the user disconnects or logs out of their desktop. If the user logs in using Leostream Connect, the client sends a Connection Close event, and you can determine if the Disconnect or Log out portion of the release plan should be executed.

You can perform actions on the desktop after the user's session is idle for the selected elapsed time. In addition, you can monitor the desktop's CPU levels to ensure that any processes the user is running come to completion before you forcefully log them out.

You can release a desktop back to its pool after a specified elapsed time since the desktop was initially assigned to the user. After the desktop is released, if the user remains logged in, the Connection Broker considers them to be *rogue*.

To avoid rogue users, forcefully log out the user when the desktop is released to its pool.

Select this option to have the Connection Broker completely delete the VM from disk as soon as the desktop is released to its pool. The Connection Broker deletes the VM only if the "Edit Desktop" page for that VM selects the "Allow this desktop to be deleted from disk" option.

2. Enter a unique name for the plan in the **Plan name** edit field.

3. To build the Release Plan for our example, in the **When User Disconnects from Desktop** section, select **after 1 hour** from the **Forced Logout** drop-down menu.

4. Click **Save**.

When using this release plan, the Connection Broker forcefully logs the user out an hour after they disconnect from their desktop. The logout event then triggers the **When User Logs Out of Desktop** section of the release plan, which releases the desktop back to its pool and removes the user's assignment to the desktop.

For more details on creating and using release plans, see the "Release Plans" section in Chapter 11 of the Connection Broker Administrator's Guide.
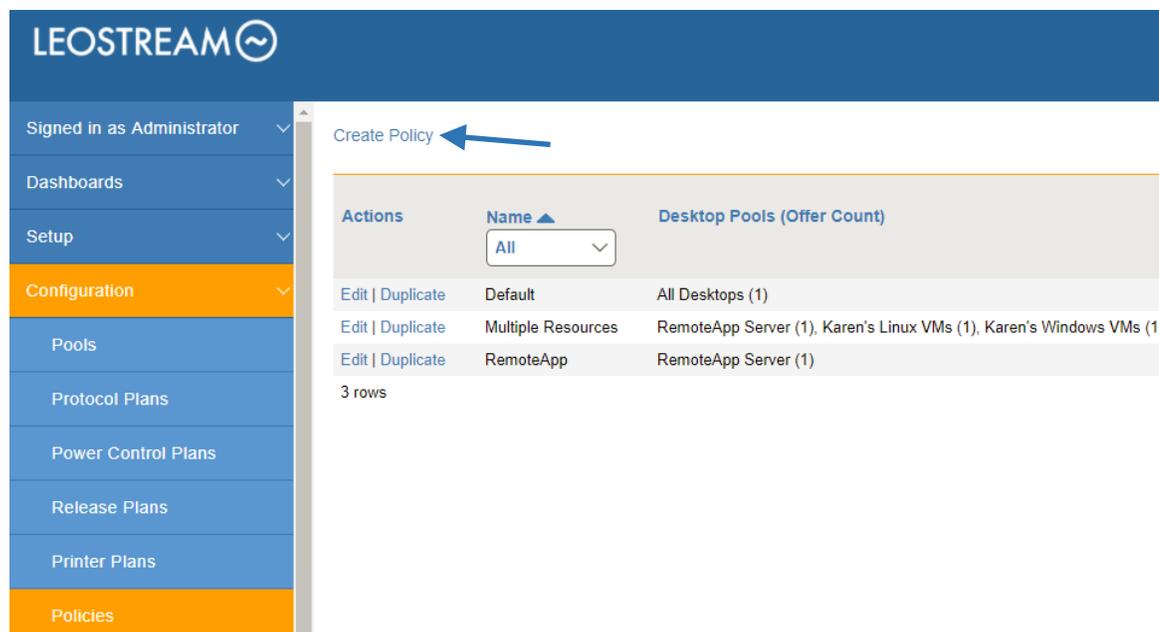
Step 3: Building User Policies

After you define your pools and plans, build policies.

💡 *The Leostream Connection Broker defines a **policy** as a set of rules that determine which pools to offer desktops from, which display protocol to use to connect to those desktops, which power control and release plans to apply to those desktops, which USB devices the user can access in their remote desktop, and more.*

The Connection Broker provides a **Default** policy that applies if no other policy exists or is applicable. The **Default** policy assigns one desktop from the **All Desktops** pool. You can create additional policies, as follows:

1. Navigate to the **> Configuration > Policies** menu.

2. Click the **Create Policy** link, shown in the following figure.

The **Create Policy** form, shown in the following figure, opens.

3. In the **General** tab, enter a name for the policy in the **Policy name** edit field. For a discussion on the remaining general policy properties, see the [Connection Broker Administrator's Guide](#).

4. Click **Save** to continue building the policy.

5. Go to the **Pool Assignments** tab.

   Click the **Add Pool Assignments** link. In the **Edit Pool Assignment** form:

   a. In the **When User Logs into Connection Broker** section, use the **Number of desktops to offer** drop-down menu to indicate the number of desktops to offer to a user of this policy.

   b. Use the **Pool** menu to select the pool to offer desktops from. When a user is offered this policy, the Connection Broker sorts the desktops in the selected pool based on the other policy settings, then offers the user the top *n* desktops from the pool, where *n* is the number selected in the **Number of desktops to offer** drop-down menu.

16

c. Scroll down to the **Plans** section and select the protocol, power control, and release plans to apply to desktops offered from this pool.

d. Click **Save**.

In a simple proof-of-concept environment, many of these settings can be left at their default values. Note that, by default, the Connection Broker does not offer a desktop to the user if the desktop does not have an installed Leostream Agent. If you want to offer desktops that do not have a Leostream Agent, select the **Yes, regardless of Leostream Agent status** option from the **Offer running desktops** drop-down menu.

For a complete description of setting up policies, see "Configuring User Experience by Policy" in the Connection Broker Administrator's Guide.

Step 4: Assigning Policies to Users

When a user logs in to the Connection Broker, the Connection Broker searches the authentication servers on the **> Setup > Authentication Servers** page for a user that matches the credentials provided by the user.

The Connection Broker then looks on the **> Configuration > Assignments** page, shown in the following figure, for the assignment rules associated with the user's authentication server. For example, if the Connection Broker authenticated the user in the LEOSTREAM domain defined on the **> Setup > Authentication Servers** page, the Connection Broker would look in the LEOSTREAM assignment rules in the following figure.

To assign policies to users in a particular authentication server, click the **Edit** link associated with that authentication server on the **> Configuration > Assignments** tab, shown in the previous figure. The **Edit Assignment** form for this authentication server appears, shown in the following figure.

By default, the Connection Broker matches the selection in the **Group** drop-down menu to the user's `memberOf` attribute in Active Directory.

If you modified your groups in Active Directory after you last signed into your Connection Broker, you must sign out and sign back in to have your Connection Broker reflect the authentication server changes.

To assign policies based on the user's `memberOf` attribute:

1. Select the group from the **Group** drop-down menu.

2. If you are using locations, select a location from the **Client Location** drop-down menu.

3. Assign a role to this group and client location pair by selecting an item from the **User Role** drop-down menu.

💡 *In Leostream, **roles** are permissions that control the actions an end user can take on their desktop and the level of access the user has to the Connection Broker Administrator Web interface. A **location** is a group of clients defined by attributes such as manufacturer, device type, OS version, IP address, etc. For more information on building roles and locations, see Chapters 10 and 13 in the [Connection Broker Administrator's Guide](#).*

4. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu.

If you need to assign roles and policies based on a different user attributes, see "Assigning Roles and Policies Based on any Attribute" in Chapter 14 of the [Connection Broker Administrator's Guide](#).

Step 5: Testing Your Connection Broker Configuration

To test your Connection Broker, ensure that users are being assigned to the correct policy, and offered the correct desktops. You can test user logins before the user has ever logged into, and been loaded into, Leostream.

1. Navigate to the **> Resources > Users** page. As users log into your Leostream environment, their user information is added to this page. You do not need to load users before they can log in.

2. Click the **Test Login** link at the top of the page, shown in the following figure.
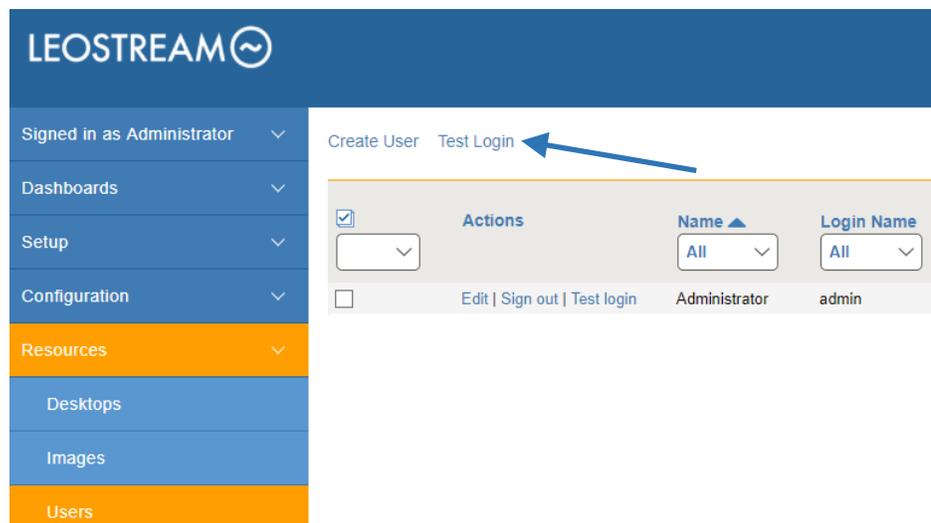
3. In the **Test Login** form that opens, enter the name of the user to test in the **User Name** edit field.

4. If you are allowing the user to specify their domain, select a domain from the **Domain** drop-down.

5. Click **Run Test**. The Connection Broker searches the authentication server for your user, and then presents a report, for example:

Test Results
User name: Maybel
Authentication server: Leostream
Domain: leostream.net
Client: Chrome/91.0 (Web Browser) at 10.110.3.40
                         (This client is in these locations: Web browsers, All)

Looking up user "Maybel":
  in authentication server "Leostream" ← **found user** (show Active Directory attributes)

Trying to match with Authentication Server Assignment rules: (edit)
    1: "memberOf" exactly matches "CN=Karen Test Sub Group,OU=Karen Test,OU=Karen Groups,DC=leostream,DC=net", location "All" ← no attribute match
    2: "memberOf" exactly matches "CN=Students,OU=Security Groups,DC=leostream,DC=net", location "All"   ← **matched**
User will have Role "User" and Policy "Default"
User must first successfully authenticate with RADIUS server "Okta RADIUS Agent" ← **PIN+token not provided**
User's role provides access to Web Client, only.

Policy: Default (edit)

No hard-assigned desktops found

Pool "All Desktops" (edit)
Including pool for all users
Looking for two desktops
Policy settings for this pool:
 - follow-me mode
 - do not allow users to change power state of offered desktops
 - offer powered-on desktops without a running Leostream Agent
 - do not offer stopped/suspended desktops
 - favor previously-assigned desktops
 - may offer desktops with pending reboot job
 - do not confirm desktop power state
 - do not power on stopped desktops
 - do not log out rogue users
 - do not attempt single sign-on into desktop console session
 - allow manual release (but Maybel's role prevents it)
 - Power control plan: Default
  - when user disconnects, do not change power state
  - when user logs out, do not change power state
  - when desktop is released, do not change power state
  - when desktop is idle, do not change power state
 - Release plan: Default
  - handle unverified user state as disconnect
  - do not release on disconnect
  - do not log user out on disconnect
  - when user logs out, release immediately
  - do not lock desktop if idle
  - do not disconnect user if desktop is idle
  - do not log user out if desktop is idle
  - do not release after initial assignment
  - if user does not log in, release
(389 total, 383 in service, 18 policy filtered, 18 pool filtered, 18 available, 8 running, 8 with an IP address)
  kdg-debian9 ← **available**, running, Leostream Agent v5.1.22.0, will offer as: "kdg-debian9", will connect via RDP (show) ← will use protocol plan "Default" associated with policy Default
  kdg-1803   ← **available**, running, Leostream Agent v7.3.13.0, will offer as: "kdg-1803", will connect via RDP (show) ← will use protocol plan "Default" associated with policy Default

Offering two desktops with this policy.

See "Testing User Role and Policy Assignment" in the Connection Broker Administrator's Guide for information on interpreting test login results.

Please complete a login test before contacting Leostream Support.